Per non ricorrere allo SCITALE

Ing. Massimo Rivalta
presidente Animac

Le attività di cyber security si applicano a diversi livelli e puntano alla protezione di computer, programmi, reti e dati. Sono richieste misure di sicurezza che si fondano su tre elementi: le persone, i processi e la tecnologia. Una triplice barriera difensiva, quindi, che protegge dalle minacce provenienti dal web. Vulnerabilità e importanza del dato.

La sicurezza sul posto di lavoro è spesso intesa come una serie di regole, articoli, leggi, atte a evitare che si verifichino infortuni. Oltre a quella dettata dall'enunciato del D.Lgs. 81/08 e ripresa più volte dalle normative di settore, esiste anche un altro tipo di sicurezza, più impalpabile e più difficile da mettere in atto proprio perché invisibile, ma per questo non meno pericolosa. Si tratta della sicurezza informatica.

La sicurezza informatica, nota anche come sicurezza digitale, è la pratica volta a proteggere le informazioni digitali, i dispositivi e le risorse personali. Compresi le informazioni personali, gli account, i file, le fotografie, e tutto quanto rappresenta la nostra sfera privata e i dati sensibili.

"C.I.A." non è soltanto, come potrebbe sembrare, l'acronimo della famosa agenzia di investigazione americana, piuttosto "C.I.A." viene spesso usato per rappresentare i tre pilastri della sicurezza informatica che sono:

- Confidenzialità: proteggere i propri segreti, garantire che solo le persone autorizzate possano accedere ai file e agli account dell'utente.
- Integrità: assicurare che le informazioni corrispondano a quanto previsto e che nessuno abbia inserito, modificato o eliminato elementi senza autorizzazione. Ad esempio, modifica dannosa di un numero in un foglio di calcolo.
- Accesso: assicurarsi di poter accedere all'informazione ai sistemi quando necessario. Un esempio di un problema di accesso potrebbe essere un attacco di tipo denial of service in cui gli attaccanti sovraccaricano il traffico di rete del sistema per rendere quasi impossibile l'accesso; oppure ransomware che crittografa il sistema e ne impedisce l'uso.

La sicurezza non un prodotto...

Anche se le app e i dispositivi di sicurezza, come il software antimalware e i firewall sono essenziali, non è sufficiente collegare questi strumenti per essere sicuri. La sicurezza digitale richiede la creazione di un insieme di processi e procedure ben ponderati, quali: backup dei dati, buone abitudini informatiche, mantenere aggiornato il software, usare password complesse e univoche, usare l'autenticazione a più fattori.

... è uno sport di squadra

Internet fa parte della quotidianità di tutti. Influenza le attività lavorative e quelle personali. Ma spesso, a causa della scarsa conoscenza dei rischi che si legano all'utilizzo di questo strumento, ci si imbatte in seri pericoli per la sicurezza informatica.

Seguire alcune semplici norme di buon senso ridurrebbe certi rischi. Un attacco di cyber security, ad esempio, potrebbe essere alla base di un furto di identità, la perdita di dati importanti e personali, a livello individuale.

Il rischio si estende anche ad enti

e istituzioni pubbliche, oppure a grandi aziende, e proteggerle risulta essenziale per garantire il buon funzionamento di tutti i servizi di una città, una regione, uno stato, oppure un'azienda, grande o piccola che sia.
In questo senso, il lavoro dei ricercatori che si occupano di minacce informatiche è di grande utilità. Le attività di cyber security si applicano a diversi livelli e puntano alla protezione di computer, programmi, reti e dati. Sono richieste misure di sicurezza che si fondano su tre elementi: le persone, i processi e la tecnologia. Una triplice barriera difensiva, quindi, che protegge dalle minacce provenienti dal web.
I dati sono beni preziosi. E possono avere un impatto decisivo su molti fronti. Per questo è importante mettere in atto strategie di protezione e sicurezza informatica.

La formazione e strategie

In ambito aziendale, la formazione del personale in tema di trattamento dei dati personali è un altro elemento chiave. Le strategie di sicurezza sono molteplici e dipendono da diversi fattori. E' importante sapere che la vulnerabilità dei dispositivi elettronici accresce il raggio di azione dei criminali del cyber spazio; devono quindi esistere precise strategie difensive: dall'identificazione di aree critiche, alla gestione dei rischi, al controllo degli accessi, alla gestione della privacy e così via.
Nell'era di Industria 4.0 e della trasmissione dei dati da un sistema industriale ad un server remoto in grado di monitorare ogni variazione di funzionamento degli impianti, l'anello debole della catena è proprio il momento del trasferimento dei dati stessi, ma non solo: anche quando i dati sono custoditi rimangono oggetto di attacchi informatici. Per questo non bisogna abbassare la guardia pensando di essere al sicuro solo perché i nostri dati raggiungono un sistema remoto dotato di aggiornate misure di sicurezza.

Il rischio

Il pericolo di perdita dei dati (o di furto, dipende dai casi) avviene in tempi e modi differenti: all'interno dell'impianto che li acquisisce dai processi produttivi, al momento in cui questi vengono inviati telematicamente al server interno aziendale o al server remoto dell'azienda esterna (magari in un paese estero) che li monitora e controlla all'interno della banca dati in cui vengono memorizzati. Un esempio di questa catena di trasferimento, monitoraggio e salvataggio è oggi rappresentato da tutti quegli impianti che sono dotati di un sistema di rilevamento e trasmissione dati (come le schede telefoniche installate all'interno dei compressori) verso un server esterno, qualunque esso sia. All'interno della stringa trasmessa, questi hanno differenti livelli di importanza. Possono rappresentare parametri di processo di un segreto industriale o racchiudere il ciclo di funzionamento del compressore o dei compressori che gestiscono una rete di aria compressa dedicata ad un prodotto o composto particolare (si può immaginare per un'azienda leader nel settore farmaceutico o chimico quanto sia importante proteggere i brevetti e tutto il sistema di risorse e di ricerca industriale), oppure semplicemente rappresentare il ciclo produttivo di un'azienda o di un impianto.

Si può intervenire?

Cosa si può fare per avere la certezza e la sicurezza che quanto immagazziniamo attraverso macchinari sempre più sofisticati sia al sicuro?
La tecnologia ci spinge ad avere macchine e sistemi sempre più complessi e non gestibili manualmente se non da preparatissimi tecnici informatici (non più solo meccanici ahimè!) e a fidarci di processi telematici che acquisiscono sempre più dati, tutti i tipi di dati. A questo punto la domanda è la seguente: siamo oggi ancora noi padroni della nostra privacy o tutto dipende dalla sicurezza interna di un sistema o dalla (in-)capacità di un pirata informatico? Sarebbe bene meditare se sia più importante perseguire un modus operandi tecnologicamente avanzato, ma vulnerabile, piuttosto che avere meno tecnologia applicata alle macchine e più sicurezza informatica.
Oggi ci preoccupiamo di mantenere riservate le informazioni personali, militari e d'affari, ma nessuno ha la certezza che le stesse siano veramente al sicuro dall'attacco di qualche cyber pirata. Forse bisognerebbe ritornare al vecchio sistema dello scitale.
Nel V secolo a.C. gli spartani inviavano gli ordini ai capi militari tramite messaggi scritti su una striscia di cuoio che, avvolta su un bastone di un diametro ben preciso (lo scitale, appunto), permetteva di leggere il testo in chiaro lungo il bastone; Giulio Cesare invece, cifrava i messaggi. Ma una via di mezzo non si può proprio avere? L'importanza del dato potrebbe essere la discriminante.
In ogni caso, un'arma che sempre abbiamo è studiare, informarci e formarci su tutti i fronti, a cominciare dalla normativa e dalla sicurezza informatica. Lo standard ISO/IEC 27002 potrebbe aiutare non poco ad approfondire i concetti della cosiddetta cyber-security.